Listing of Claims:

1. (Original) A network comprising:

IPsec processing apparatuses, which use an IPsec (Internet Protocol security protocol) for securing security on the Internet path in the case where different two centers communicate via the Internet; and

an IPsec setting server apparatus, which manages IPsec settings of said IPsec processing apparatuses,

wherein said IPsec setting server apparatus includes means for collectively managing policies of said IPsec to be applied between first and second IPsec processing apparatuses.

2. (Original) The network according to claim 1,

wherein said IPsec setting server apparatus includes means for specifying policies of said IPsec to be applied between said first and second IPsec processing apparatuses based upon contents of a request message for communication between said first and second IPsec processing apparatuses received from said first IPsec processing apparatus.

3. (Original) The network according to claim 2,

wherein said IPsec setting server apparatus includes means for, upon receiving the request message, transmitting a request startup message to said second IPsec processing apparatus, which is an opposite party of communication of said first IPsec processing apparatus which has transmitted the request message, in order to cause said second IPsec processing apparatus to transmit a request message for the communication.

4. (Original) The network according to claim 3,

wherein said IPsec setting server apparatus includes means for, when there is no response to the request startup message, notifying said first IPsec processing apparatus that there is no response from said second IPsec processing apparatus.

5. (Original) The network according to claim 2,

wherein said IPsec setting server apparatus includes means for generating SA (Security Association) parameters to be required in the IPsec communication from contents of

the request message and contents of the policies of said IPsec to be applied to the communication.

6. (Original) The network according to claim 2,

wherein said IPsec setting server apparatus includes means for sending a distribution message including at least the policies of said IPsec and the SA parameters in response to the request message.

7. (Original) The network according to claim 1,

wherein said IPsec setting server apparatus includes means for generating a common secret key to be used in encryption and authentication of said IPsec and means for distributing the generated common secret key to said IPsec processing apparatus.

8. (Original) An IPsec setting server apparatus managing IPsec setting of IPsec processing apparatuses, which use an IPsec (Internet Protocol security protocol) for securing security on the Internet path in the case where different two centers communicate via the Internet,

wherein said IPsec setting server apparatus includes means for collectively managing policies of said IPsec to be applied among sad IPsec processing apparatuses.

9. (Original) The IPsec setting server apparatus according to claim 8,

wherein said IPsec setting server apparatus includes means for specifying policies of said IPsec to be applied between an IPsec processing apparatus and another IPsec processing apparatus based upon contents of a request message for communication between said IPsec processing apparatus and another IPsec processing apparatus received from said IPsec processing apparatus.

10. (Original) The IPsec setting server apparatus according to claim 9,

wherein said IPsec setting server apparatus includes means for, upon receiving the request message, transmitting a request startup message to an IPsec processing apparatus, which is an opposite party of communication of an IPsec processing apparatus which has transmitted the request message, in order to cause said IPsec processing apparatus of the opposite party of communication to transmit a request message for the communication.

11. (Original) The IPsec setting server apparatus according to claim 10,

wherein said IPsec setting server apparatus includes means for, when there is no response to the request startup message, notifying said IPsec processing apparatus which has transmitted the request message that there is no response from said IPsec processing apparatus of the opposite party of communication.

12. (Original) The IPsec setting server apparatus according to claim 9,

wherein said IPsec setting server apparatus includes means for generating SA (Security Association) parameters to be required in the IPsec communication from contents of the request message and contents of the policies of said IPsec to be applied to the communication.

13. (Original) The IPsec setting server apparatus according to claim 9,

wherein said IPsec setting server apparatus includes means for transmitting a distribution message including at least the policies of said IPsec and the SA parameters in response to the request message.

14. (Original) The IPsec setting server apparatus according to claim 8,

wherein said IPsec setting server apparatus includes means for generating a common secret key to be used in encryption and authentication of said IPsec and a function for distributing the generated common secret key to said IPsec processing apparatus.

15. (Original) An IPsec processing apparatus using an IPsec (Internet Protocol security protocol) on the Internet,

wherein said IPsec processing apparatus includes means for, upon receiving a packet to which said IPsec should be applied, judging whether or not to inquire a setting for said IPsec to be collectively managed in an IPsec setting server apparatus from said IPsec setting server apparatus.

16. (Original) The IPsec processing apparatus according to claim 15,

wherein said IPsec processing apparatus includes means for transmitting a request message for communication with another IPsec processing apparatus to said IPsec setting server apparatus in order to acquire a setting for said IPsec.

17. (Original) The IPsec processing apparatus according to claim 16,

wherein, upon receiving a request startup message for causing said IPsec processing apparatus to transmit the request message from said IPsec setting server apparatus, said IPsec processing apparatus transmits the request message.

18. (Original) The IPsec processing apparatus according to claim 15,

wherein said IPsec processing apparatus includes means for setting an SPD, in which policies for applying said IPsec is recorded, and an SAD, in which an SA (security Association) necessary for subjecting an individual kind of communication to processing of said IPsec, based upon a distribution message received from said IPsec setting server apparatus.

19. (Original) The IPsec processing apparatus according to claim 15,

wherein said IPsec processing apparatus includes means for acquiring a common secret key to be used in encryption and authentication of said IPsec from said IPsec setting server apparatus.

20. (Original) The IPsec processing apparatus according to claim 15,

wherein said IPsec processing apparatus includes means for retransmitting the request message to said IPsec setting server apparatus and acquiring new setting information before a term of validity of the SA expires.

21. (Original) An IPsec setting method for a network which comprises: IPsec processing apparatuses, which use an IPsec (Internet Protocol security protocol) for securing security on the Internet path in the case where different two centers communicate via the Internet; and an IPsec setting server apparatus, which manages IPsec settings of said IPsec processing apparatuses,

wherein said IPsec setting server apparatus includes a step of collectively managing policies of said IPsec to be applied among said IPsec processing apparatuses.

22. (Original) The IPsec setting method according to claim 21,

wherein said IPsec setting server apparatus includes a step of specifying policies of said IPsec to be applied between an IPsec processing apparatus and another IPsec processing apparatus based upon contents of a request message for communication between said IPsec processing apparatus and another IPsec processing apparatus received from said IPsec processing apparatus.

23. (Original) The IPsec setting method according to claim 22,

wherein said IPsec setting server apparatus includes a step of, upon receiving the request message, sending a request startup message to an IPsec processing apparatus, which is an opposite party of communication of an IPsec processing apparatus which has transmitted the request message, in order to cause said IPsec processing apparatus of the opposite party of communication to transmit a request message for the communication.

24. (Original) The IPsec setting method according to claim 23,

wherein said IPsec setting server apparatus includes a step of, when there is no response to the request startup message, notifying said IPsec processing apparatus which has transmitted the request message that there is no response from said IPsec processing apparatus of the opposite party of communication.

25. (Original) The IPsec setting method according to claim 22,

wherein said IPsec setting server apparatus includes a step of generating SA (Security Association) parameters to be required in the IPsec communication from contents of the request message and contents of the policies of said IPsec to be applied to the communication.

26. (Original) The IPsec setting method according to claim 22,

wherein said IPsec setting server apparatus includes a step of transmitting a distribution message including at least the policies of said IPsec and the SA parameters in response to the request message.

27. (Original) The IPsec setting method according to claim 21,

wherein said IPsec setting server apparatus includes a step of generating a common secret key to be used in encryption and authentication of said IPsec and a step of distributing the generated common secret key to said IPsec processing apparatus.

28. (Original) The IPsec setting method according to claim 21,

wherein, upon receiving a packet to which said IPsec should be applied, said IPsec processing apparatus judges whether or not to inquire a setting for said IPsec to be collectively managed in an IPsec setting server apparatus from said IPsec setting server apparatus.

29. (Original) The IPsec setting method according to claim 21,

wherein said IPsec processing apparatus transmits a request message for communication with another IPsec processing apparatus to said IPsec setting server apparatus in order to acquire a setting for said IPsec.

30. (Original) The IPsec setting method according to claim 21,

wherein said IPsec processing apparatus sets an SPD, in which policies for applying said IPsec is recorded, and an SAD, in which an SA (Security Association) necessary for subjecting an individual kind of communication to processing of said IPsec, based upon a distribution message received from said IPsec setting server apparatus.

31. (Original) The IPsec setting method according to claim 21,

wherein said IPsec processing apparatus acquires a common secret key to be used in encryption and authentication of said IPsec from said IPsec setting server apparatus.

32. (Original) The IPsec setting method according to claim 21,

wherein said IPsec processing apparatus resends the request message to said IPsec setting server apparatus and acquires new setting information before a term of validity of the SA expires.